

# Eine Firewall sieht rot...

gateProtect High End Firewall Server

In den vergangenen Ausgaben haben wir uns ausführlich mit dem Thema Sicherheit bei Computern im trauten Eigenheim beschäftigt. Sie haben erfahren, wieso gerade auch Ihr System für kriminelle Elemente so einiges an begehrenswerten Daten bietet und wurden mit realen Angriffsszenarien konfrontiert. All dies sorgt auch und gerade in Zeiten der Wirtschaftskrise für zusätzliche Verluste - auch im geschäftlichen Bereich. Da virtuelle Angriffe ein Unternehmen ungleich mehr schädigen können, sollte man sich eigentlich gerade dort um den bestmöglichen Schutz kümmern. Dass die Praxis anders aussieht, lesen sie im folgenden Artikel. Und dass es mit der im Anschluss vorgestellten Appliance eine brauchbare Alternative gibt, ebenso.

DI (FH) Christian Sudec



Echt fesch, die Firewall-Serie GPA von gateProtect.

Um das Für und Wider dieses Stücks Hardware besser abschätzen zu können, gilt es, etwas weiter auszuholen. Denn während es beim Privatanwender mit der Installation einiger Software-Tools wie Virens Scanner, Firewall und Webfilter getan ist, ist diese Vorgehensweise für Unternehmen so nicht praktikabel, da hier die genannten Vorkehrungen einfach nicht mehr ausreichen. Der Administrator muss also bereits in größeren Dimensionen denken, obwohl es sich vielleicht nur um ein Kleinunternehmen mit weniger als 10 Mitarbeitern handelt. Der Grund liegt in verschiedenen Komponenten, die sich in der Regel bei einem Privatanwender nicht mehr finden. Ob es sich dabei um einen Webserver für den Firmenauftritt im Internet oder einen zusätzlichen Fileserver mit Datensynchronisation zur Filiale handelt, ist unerheblich. Fakt ist, dass sowohl diese Dienste, als auch ihr Zusammenspiel im LAN, als auch die Netzwerkstruktur selbst überwacht werden müssen. Andernfalls ist der Schutz der Unternehmensdaten nicht gewährleistet. Schließlich könnten hier nicht nur wirklich relevante Daten in die falschen Hände gelangen, auch der so entstehende Schaden würde sich (leider meist über Gehaltskürzungen oder Abschlüsse) indirekt auf die Mitarbeiter auswirken und so mehr Leben in Mitleidenschaft ziehen als bei einem Privatanwender.

Damit ich Ihnen die Hürden bei der Absicherung eines Unternehmens besser präsentieren kann, bleiben wir bei unserem Kleinbetrieb eines beliebigen Gewerbes mit besagten 10 Mitarbeitern. Diese Unternehmensart ist in Österreich sehr häufig anzutreffen und agiert im Bereich der IT-Anschaffungen und Wartung - auf Grund meiner langjährigen Erfahrung - faktisch nach folgendem Prinzip: der Chef gibt nur das Notwendigste für die Erhaltung der EDV-

Infrastruktur aus. Die Arbeitsstationen hinken der aktuellen Technik immer hinterher. In der Regel etwa 3-6 Jahre, da meist ein Abschreibungsintervall übersprungen wird. Und Lizenzen werden sowieso nur dann angeschafft, wenn die dazugehörige Software ohne Aktivierung nicht mehr funktionieren würde oder regelmäßige Updates sich direkt auf die Finanzen/Produktion auswirken. Letzteres wäre z.B. bei FiBu-Anwendungen und Maschinensteuerungen der Fall.

Der IT-Fachmann wird grundsätzlich nur dann gerufen, wenn ‚Feuer am Dach‘ ist - sprich: es geht jetzt irgendetwas nicht. Per Brief eintreffende Hinweise, dass ein Generalcheck empfehlenswert wäre, landen ebenso wie die Aufforderung zum Jahresservice des Autohändlers in der Ablage ‚Ferner liefern‘, auch Papierkorb genannt. Ferner müssen EDV-Projekte schnellstens umgesetzt werden, da entweder die Konkurrenz ‚auch schon so etwas hat‘ (z.B. Webseite, zentral synchronisierter Kalender, etc.) oder immer mehr Leute/Kunden/Behörden danach fragen (z.B. e-Mail-Adresse; Preislistendownload, etc.). Entweder kommt nun in Folge der billigste Anbieter zum Zug oder der hauseigene IT-Verantwortliche wird beauftragt, das Ganze so billig wie möglich zu realisieren. Ab hier trennen sich die Wege. Je nachdem, wie kompetent die jeweilige Person die Angelegenheit umsetzt. Entweder erhält der Chef eine kostenlose Lösung auf Basis von Open Source oder aber wieder die Raubkopie einer ‚einfacher‘ zu bedienenden kommerziellen Software. Egal welcher Weg nun eingeschlagen wird, so treffen sich beide wieder. Und zwar nach dem (hoffentlich) erfolgreichen Abschluss bei der Schlussbemerkung des Chefs: „Das sollte jetzt die nächsten Jahr(zehn)te problemlos laufen!“

Soweit zu unserer typischen Kleinfirma, wie sie so nicht nur im Alpenland existiert. Man könnte hier noch unzählige weitere Studien betreiben und Hypothesen aufstellen, aber konzentrieren wir uns jetzt auf die Fakten, die wir aus der obigen Schilderung erhalten. Erstens besitzen die Arbeitsstationen unterschiedliche Hardware - teils begründet durch die verschiedenen Anschaffungsperioden, teils durch diverse ‚Notfallreparaturen‘. Somit haben die Einzelrechner nicht nur unterschiedliche Treiber, sondern auch eine differierende Performance. Dies führt dazu, dass ein Programm, welches auf Computer A klaglos seinen Dienst verrichtet, dies nicht unbedingt auf Computer B tun wird. Und das gilt folglich nicht nur für Unternehmenssoftware, sondern eben auch für Security-Suiten.

Da es keinen Administrator gibt, der permanent vor Ort ist, arbeiten praktisch alle Mitarbeiter mit vollen Rechten am PC - nichts ist störender (und kostspieliger), als den EDV-Betreuer bei jeder kleinen Änderung (z.B. „Windows-Energieschema ändern, dass sich der Monitor, auf dem die Produktdemo läuft, nicht abschaltet“) zu rufen. Als Folge wird von der Sekretärin schnell das Schulprogramm vom Junior drauf installiert, damit dieser auf dem Firmendrucker seine Zeichnungen ausdrucken kann; der Lagerleiter hat wiederum unzählige Spiele auf der Festplatte; etc.

Die ‚offiziell‘ genutzten Anwendungen hingegen sind wegen der fehlenden Lizenzen nicht Update-berechtigt und reißen mit jedem Tag mehr Lücken ins System, die mit Hilfe von manipulierten Dokumenten ausgenutzt werden. Und da eben mit dem Administrator-Account gearbeitet wird, gibt es - außer einem lokal installierten Scanner (der nicht regelmäßig aktualisiert wird) - keine weiteren Hürden vor einer ‚feindlichen Übernahme‘.

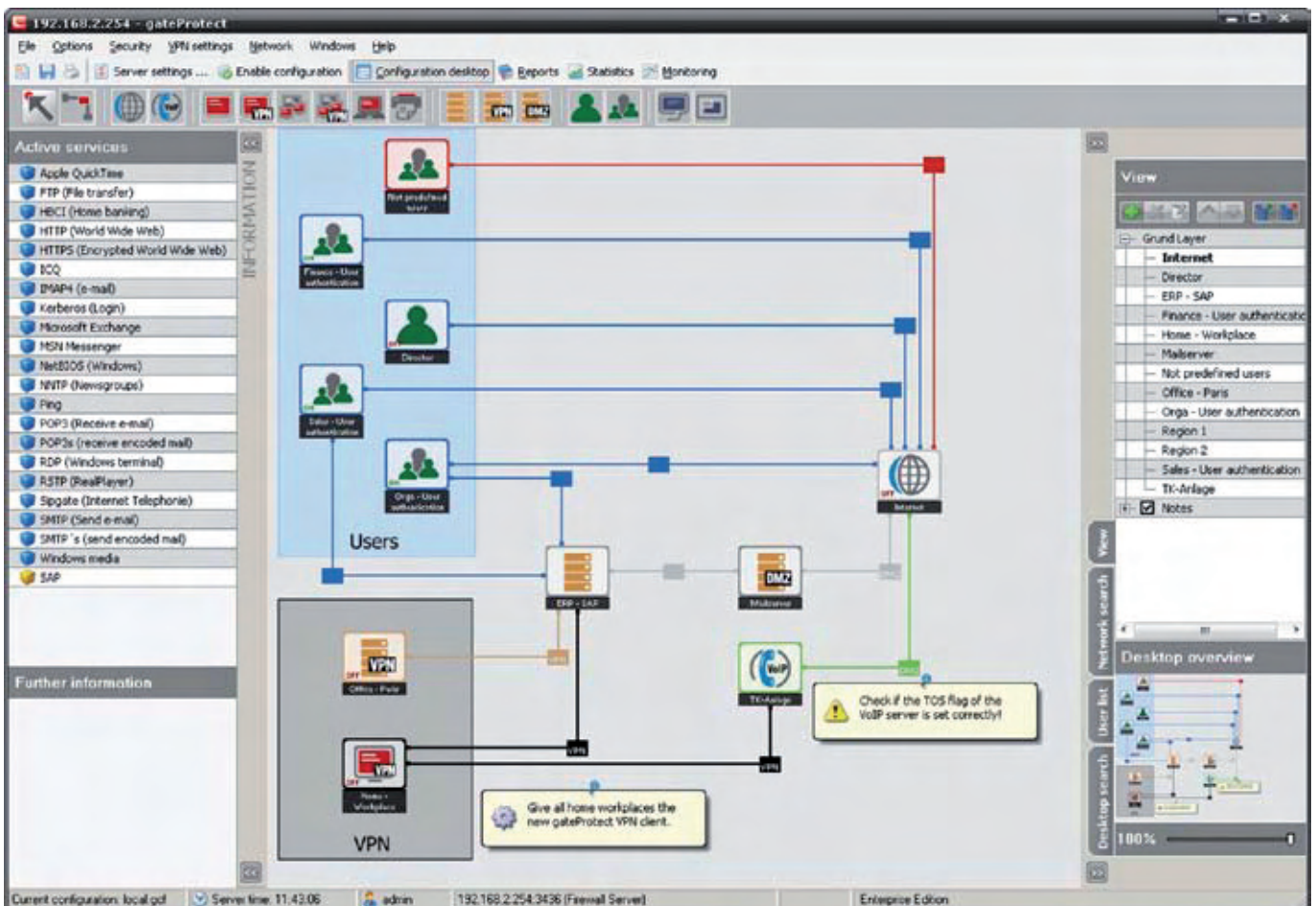
Ähnliches gilt für die Geräte aus obigen Projekten, die permanent laufen und daher nicht mehr angegriffen (im Sinne von berührt) werden (dürfen). Auch wenn Linux drauf läuft, so ist das kein Garant für Sicherheit und so werden diese allzu gerne angegriffen (im Sinne von attackiert). Der Vorteil für den Eindringling: er bleibt oft Wochen unentdeckt!

Auf Grund der unterschiedlichen Dienstleister, die immer wieder Komponenten dazu stecken bzw. erweitern, gibt es keine einheitliche Dokumentation des Netzes. Meist wird zudem DHCP eingestellt, so dass neue Geräte schnell und unkompliziert eine IP-Adresse erhalten. Gleiches gilt allerdings auch, wenn ein Angestellter seinen Privatlaptop

ins LAN hängt. Spätestens dann hat man überhaupt keine Kontrolle mehr darüber, was im Netzwerk abgeht. Sprich: welche Rechner mit welchen Adressen vorhanden sein sollten und welche nicht. Eine Konsolidierung dieser Struktur (inklusive Absicherung) kommt leider einer Sisyphus-Arbeit gleich, weshalb dies ohnehin gescheut wird.

Security-Suiten oder diverse Einzelprodukte können daher kaum auf allen Arbeitsstationen identisch eingesetzt werden. Zum einen aus oben genannten Performance- und Update-Gründen, zum anderen, weil diese Tools nur den lokalen Computer überwachen und ferner auch nur für einen Betriebssystem-Typ existieren. In diese Presche versuchen nun die so genannten Appliances zu springen. Hinter diesem Namen verbirgt sich ein relativ unscheinbares Stück Hardware. Meist handelt es sich um Gehäuse für den Rack-Einbau, die teilweise abgestimmte PC-Komponenten, teilweise aber auch spezielle Chipsätze beinhalten. Gleiches gilt für das Betriebssystem: entweder Standardware oder Spezial-OS. Egal welche Kombination verwendet wird, sie wird explizit an ihre zukünftige Aufgabe angepasst. Ein weiteres Augenmerk liegt dabei auf der Einfachheit. Dies gilt für die erste Einrichtung und auch für die spätere Bedienung. Ziel ist es, dass auch jemand mit nicht so fundierten IT-Kenntnissen die Appliance problemlos in Betrieb nehmen und deren Ausgaben korrekt interpretieren kann. Damit werden mehrere Fliegen mit einer Klappe geschlagen: 1. Fehler seitens des Anwender bei der Installation sind ausgeschlossen, da es out-of-the-box laufend geliefert wird; 2. das System ist schlank, stabil und sicher, da es nur die notwendigen Dienste anbietet und somit nur eine minimale Angriffsfläche liefert; 3. die anwenderfreundliche

*Administrator-Oberfläche mit Mail- und Webserver in jeweils einer DMZ.*





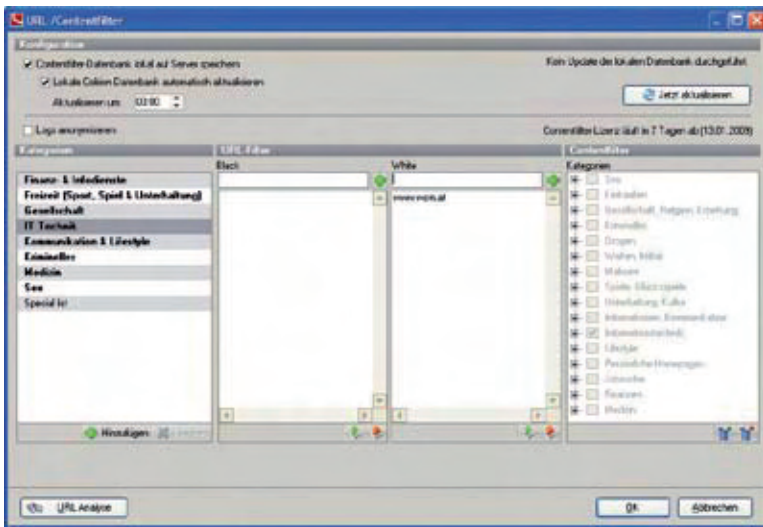
hin und geben im erscheinenden Dialogfeld die IP-Adresse des Servers ein. Nun noch auswählen, auf welcher LAN-Buchse er angesteckt ist, dem Internet-Objekt den Zugriff

nen. Neben einer Inhaltssperre lässt sich auf die gleiche Art (diesmal jedoch für die Arbeitsstationen) auch eine Zeitsperre verwirklichen, welche zum Beispiel privates Surfen nach Ende der Geschäftszeit erlaubt (siehe auch Proxies weiter unten).

Wie eben beschrieben, lässt sich die gesamte Konfiguration analog durchführen: benötigte Symbole auf die Zeichenfläche ziehen, das angezeigte Dialogfeld ausfüllen und mit zusätzlichen Verbindern an beliebige weitere Objekte koppeln. Jetzt besteht die Möglichkeit, noch einmal alles zu überprüfen, bevor ein Druck auf F9 Ihr grafisches Regel-Kunstwerk in maschinenlesbare Form übersetzt und auf die Appliance transferiert, wo es sofort zum Einsatz kommt.

Kommen wir zur Aufzählung der restlichen Features, die sich über den Client komfortabel einstellen lassen. Neben den üblichen richtungsbasierten Filtern, bieten nahezu alle gateProtect-Typen ein vollständiges IDS (Intrusion Detection System), um den Datenverkehr auf Angriffsmuster zu scannen. Zusätzlich stehen Application Level Filter und Proxies für die wichtigsten Internet-Dienste (HTTP(S), FTP, SMTP, POP3 & VoIP) zur Verfügung, welche die übertragenen Daten auf die Einhaltung der Firmenpolitik hin überwachen. Dazu kann man auf entsprechende Datenbanken mit bereits klassifizierten URLs zugreifen oder eigene URL-Listen erstellen. Die Proxies können natürlich auch transparent (ohne dass der Anwender etwas merkt) betrieben werden.

Vor allem für größere Installationen interessant: User auf der Firewall können gegen bestehende Datenbanken (Active Directory, openLDAP, etc.) authentifiziert werden,



URL-Filter-Einstellungen werden hier vorgenommen.

erlauben (und zwar nur Webdienste, die als Vorlage bereits vorhanden sind) – Fertig! Ab sofort wird eine Verbindung zwischen Internet und Webserver angezeigt. Ein Doppelklick auf diese zeigt uns in grafischer Form, von wo bzw. wohin der Datenfluss erlaubt ist. Alle anderen Pakete bleiben verboten und werden ohne viel Aufsehen gekübelt, wie es sich für eine gute Firewall gehört. In einem weiteren Tabellenreiter können zudem Filter gesetzt werden, so dass nur arbeitsrelevante Inhalte über den Webserver wandern und Mitarbeiter keine Spiele für die Kollegen ablegen kön-

## Die neue 500 Mbit Firewall FortiGate 110C

500 Mbit Firewall / 100 Mbit IPSec VPN / max. 400.000 Sessions  
1.500 VPN Tunnel / 4.000 Policies  
10 konfigurierbare Ports\*  
\* 2x 10/100/1000 Mbit, 8x 10/100 Mbit



Der neue Fortinet ASIC sorgt für höchste Performance

**ab EUR 2.245,- / 3.235,-\*\***

\*\*inkl. 12m AV-, IPS-, WEB-Filter und SPAM-Filter- Updates - exkl. MwSt.!



<http://corex.at/Produktinfos/FGT110C.pdf>

- ✓ Traffic-Shaping
- ✓ Anti-SPAM
- ✓ Web-Filter
- ✓ Anti-Virus / Anti-Spyware
- ✓ IDS / IPS
- ✓ Firewall
- ✓ IPSec / SSL VPN

**COREX**  
EDV-Dienstleistungen GmbH

<http://www.fortinet.com>  
<http://www.corex.at>  
<mailto:fortinet@corex.at>

**FORTINET**

so dass die Einrichtung zusätzlicher Benutzerkonten nicht notwendig ist und später vielleicht sogar ein Single-Sign-On realisiert werden kann. Sprich: die Benutzer melden sich einmal an und die Appliance kümmert sich um alle weiteren Authentifizierungen: darf sich der Benutzer grundsätzlich am Webserver anmelden, so geschieht dies ab jetzt automatisch, sobald er neue Inhalte auf die Homepage spielen will. Vorbei die Zeiten, wo man sich unzählige Passwörter merken musste.

Mail- bzw. Spam-Filter gehören natürlich ebenso zur Ausstattung wie die Option, Heimarbeiter mittels VPN in das Firmen-LAN zu lassen. Weiters kann über eine extra zu erwerbende Kaspersky-Lizenz der Datenverkehr zwischen den Hosts auf Viren kontrollieren. Infektionen werden somit auf Datentransferebene verhindert. Für alles gilt weiterhin: Einrichtung wie gehabt per Drag-and-Drop bzw. über die erweiterten Eigenschaften einer Verbindung.

Netzwerkprofis werden sich wiederum über Funktionen zur Hochverfügbarkeit und zum Traffic Shaping mit QoS (Quality of Service) freuen. Letzteres ermöglicht die Zuweisung von definierten Bandbreiten beim Datenverkehr für bestimmte Dienste und Anwender. Damit es beispielsweise bei der Internet-Telefonie zu keinen Aussetzern kommt, nur weil Mayer aus der Forschung wieder mal ein riesengroßes Update für sein Statistik-Tool saugt.

Wenn wir schon bei Statistiken sind, so werfen wir gleich mal einen Blick auf den gleichnamigen Menüpunkt in unserem Client. Hier findet der Chef eine vollständige Auflistung der angesurften Webseiten, sortiert nach Tageszeit. Der Administrator wiederum sieht auf einen Blick, welche Viren aufgetreten sind und wie sich alle Dienste prozentual die Bandbreite teilen. Der Abschnitt ‚Berichte‘ listet noch wichtige Ereignisse aus dem laufenden Betrieb, während schließlich unter ‚Monitoring‘ die technische Seite (Platten- und Prozessor-Auslastung, NIC-Traffic, etc.) der Appliance nicht zu kurz kommt.

## Fazit

Ich gebe es zu, anfangs dachte ich: „Schon wieder eine Firewall-Appliance, die versucht, Open Source hinter einen ansprechenden GUI zu verstecken.“ Normalerweise wird hierfür X-Windows oder ein Web-Interface verwendet - mit Ergebnissen, die mich nicht so vom Hocker reißen. Auch grafische Frontends wie fwbuilder, nerven mich eher, so dass ich bisher mit meinen Skripten auf der Shell blieb. Daher war ich auch bei der Usability der gateProtect High End Firewall mehr als skeptisch. Doch weit gefehlt. Die Idee, die Konfiguration auf Windows auszulagern und dort alle Design-Register zu ziehen, ist genau das, was ich mir schon lange gewünscht habe. User A braucht einen VPN-Zugang? Ein paar Klicks später ist er fertig! Hut ab, denn hier haben es die Hersteller geschafft, zwei Welten ideal miteinander zu verbinden und dem Administrator ein mächtiges Tool zu liefern, mit dem er die LAN-Struktur - wie eingangs erwähnt - wirklich überblicken kann. Sofern er Kenntnisse zu TCP/IP und der Benutzer- und Rechteverwaltung besitzt. Ein normaler Anwender, der vom Chef zum IT-Verwalter abkommandiert wird, wird trotz der deutschen Oberfläche eher ratlos vor selbiger sitzen.

Somit bleibt nur noch zu sagen, dass Rot die einzige richtige Farbe für die gateProtect ist, da sie faktisch den Ferrari unter den Firewall-Appliances darstellt! ▣



gateProtect High End  
Firewall GPA-250

zur Verfügung gestellt von:

bluechip Computer AG

Hersteller: gateProtect AG

URL: <http://www.gateprotect.de>

Ein Blick ins „Rat & Tat-Forum“ auf [www.wcm.at](http://www.wcm.at) lohnt immer!

Angeführte Preise inkl. MwSt. ab Lager Perchtoldsdorf. Stand eine Woche vor Erscheinen des Inserats, gültig solange der Vorrat reicht.

©2008 E.Weinzettl

## Speed Up Your Net!



Ihr Netzwerk liegt darnieder? Die Verkabelung leidet an Altersschwäche, der Server ist schon lange überfordert? Wir können helfen. Wir liefern nicht nur Workstations für Office, CAD und Bildbearbeitung sowie leistungsfähige Server, sondern auch stabile und hochperformante Netzwerkkomponenten. Wenn Sie Performance im Netz benötigen, können Sie auch komplette, strukturierte Verkabelung sowie kompetenten Netzwerksupport von uns ordern. Derzeit sind unsere Netzwerktechniker im Einsatz. Morgen vielleicht auch bei Ihnen. Kontaktieren Sie uns unter 01 244 0058 und verlangen Sie Herrn Weinzettl.

A-2380 Perchtoldsdorf, Wienergasse 32, Tel. 01/244 0058, Fax 01/244 0070  
email [office@i-design.at](mailto:office@i-design.at), <http://i-design.at>, Öffnungszeiten: Montag-Freitag 10-18:30 Uhr

**i-design**